PATENT
Attorney's Docket No. **COS99070**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	**MAIL STOP APPEAL BRIEF - PATENTS**
Thomas J. HERDER	)	Group Art Unit: 2134
Application No.: 09/627,558	)	Examiner: C. Brown
Filed: July 28, 2000	)	
For: SECURE TRANSACTION CARD USING BIO-METRICAL VALIDATION	)	

United States Patent & Trademark Office
Customer Service Window, Mail Stop Appeal Brief - Patents
Randolph Building
401 Dulany Street
Alexandria, Virginia 22314

APPEAL BRIEF

This Appeal Brief is submitted in response to the non-final Office Action, dated October 11, 2006, which re-opened prosecution of the present application, and in support of the Notice of Appeal, filed February 12, 2007.

I. REAL PARTY IN INTEREST

The real party in interest in this appeal is MCI, LLC.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

Appellant is unaware of any related appeals, interferences or judicial proceedings.

III. STATUS OF CLAIMS

Claims 1-22 are pending in this application. Claims 1-22 were rejected in the Office Action, dated October 11, 2006, and are the subject of the present appeal. These claims are reproduced in the Claim Appendix of this Appeal Brief.

IV. STATUS OF AMENDMENTS

An After Final Amendment was filed subsequent to the final Office Action, dated April 20, 2006. An Advisory Action, dated May 5, 2006, indicated that the After Final Amendment was considered, but did not place the application in condition for allowance. Furthermore, no indication was made regarding the entry of the After Final Amendment in the non final Office Action, dated October 11, 2006. Accordingly, for the purposes of this Appeal Brief, the After Final Amendment dated April 20, 2006 is presumed to have not been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In the paragraphs that follow, each of the independent claims that is involved in this appeal and each dependent claim that is argued separately will be recited followed in parenthesis by examples of where support can be found in the specification and drawings.

Independent claim 1 recites a method of validating a user for a transaction to be effectuated by using a transaction card (e.g., pg. 7, lines 7-12). The method includes configuring a biometric profile for said user the biometric profile including a plurality of biometric samples received from the user, where the plurality of biometric samples correspond to a plurality of questions (e.g., Fig. 2, block 202, pg. 9, lines 8-13). The biometric profile is associated with an indicium assigned to said transaction card (e.g., Fig. 2, block 204, pg. 10, lines 8-16). The user is biometrically interrogated when the transaction is attempted by the user, where the biometrical interrogation includes querying the user for a biometric response associated with a randomly selected one of the plurality of questions (e.g., Fig. 2, block 210, pg. 11, lines 14-19). The biometric response generated with respect to said user in response to the biometrical interrogation is monitored and it is determined if the biometric response matches a biometric sample in the biometric profile corresponding to the randomly selected one of said plurality of questions (e.g., Fig. 2, block 212, pg. 11, lines 19-22). If so, the user is approved for the transaction (e.g., Fig. 2, block 214, pg. 12, lines 6-8).

Independent claim 8 recites a method of validating a user for a call to be effectuated over a Public Switched Telephone Network (PSTN) using a calling card (e.g., pg. 7, lines 7-12). The method includes configuring a personalized profile for said user, said personalized profile including a plurality of voice samples elicited from said user in response to a plurality of personalized questions directed to said user (e.g., Fig. 2, block 202, pg. 9, lines 8-13); associating said personalized profile with an indicium assigned to said calling card (e.g., Fig. 2, block 204, pg. 10, lines 8-16); determining if a voice verification is needed with respect to said user when said call is attempted by said user

(e.g., Fig. 2, block 208, pg. 11, lines 3-7); if so, querying said user for a voice response to a question that is randomly selected from said plurality of personalized questions (e.g., Fig. 2, block 210, pg. 11, lines 14-19); verifying if said voice response matches a corresponding voice sample in said voice profile (e.g., Fig. 2, block 212, pg. 11, lines 19-22); and if so, approving said user for said call involving said calling card (e.g., Fig. 2, block 214, pg. 12, lines 6-8).

Independent claim 16 recites an access control system for use with a transaction-card-based scheme. The system includes a network (e.g., Fig. 3, 300, pg. 12, lines 14-17) operable with a terminal (e.g., Fig. 3, 304A-304C, pg. 12, lines 17-19), said terminal (e.g., 304A-304C) for interacting with a user (e.g., Fig. 3, 106) in association with a transaction card; a controller (e.g., Fig. 3, 322, pg. 13, lines 20-22), disposed in the network (e.g., 300) to query said user (e.g., 106) when said user attempts a transaction using said transaction card; a server (e.g., Fig. 3, 324, pg. 14, lines 1-11) disposed in the network (e.g., 300), said server (e.g., 324) responding to messages from said controller (e.g., 322) with respect to querying said user (e.g., 106); and a profile database (e.g., Fig. 3, 320) coupled to said server (e.g., 324), said profile database (e.g., 320) having a plurality of biometric samples inherently coupled to said user (e.g., 106), wherein said plurality of biometric samples relate to a plurality of questions, and wherein said biometric samples are associated with an indicium assigned to said transaction card such that when said user (e.g., 106) attempts said transaction, said controller (e.g., 324) queries said user (e.g., 106) for a response relating to a randomly selected one of the biometric samples (e.g., Fig. 4, 420, pg. 18, lines 13-15) and if said response does not match a corresponding entry in said profile database (e.g., 320, Fig. 4, 444, pg. 20, lines 13-14),

access is denied to said user for said transaction (e.g., Fig. 4, block 446, pg. 20, lines 20-21).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1-3 and 5 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over BUFFAM (U.S. Patent No. 6,185,316) in view of KANEVSKY et al. (U.S. Patent No. 5,897,616).

B. Claim 4 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over BUFFAM (U.S. Patent No. 6,185,316) in view of KANEVSKY et al. (U.S. Patent No. 5,897,616), and further in view of FUJIMOTO (U.S. Patent No. 5,893,057).

C. Claims 6 and 7 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over BUFFAM (U.S. Patent No. 6,185,316) in view of KANEVSKY et al. (U.S. Patent No. 5,897,616) and further in view of GLAZE (U.S. Patent No. 6,320,974).

D. Claims 8-10 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over BUFFAM (U.S. Patent No. 6,185,316) in view of KANEVSKY et al. (U.S. Patent No. 5,897,616), and further in view SAWYER (U.S. Patent No. 6,324,271).

E. Claim 11 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over BUFFAM (U.S. Patent No. 6,185,316) in view of KANEVSKY et al. (U.S. Patent No. 5,897,616), further in view of SAWYER (U.S. Patent No. 6,324,271), and still further in view of FUJIMOTO (U.S. Patent No. 5,893,057).

F. Claims 12-15 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over BUFFAM (U.S. Patent No. 6,185,316) in view of SAWYER (U.S.

Patent No. 6,324,271), further in view of CHMAYTELLI (U.S. Patent No. 6,542,729), and still further in view of WEISS (U.S. Patent No. 4,998,279).

G. Claims 16-22 under 35 U.S.C. § 103(a) as being unpatentable over BUFFAM (U.S. Patent No. 6,185,316) in view of KANEVSKY et al. (U.S. Patent No. 5,897,616), further in view of SAWYER (U.S. Patent No. 6,324,271), and further in view of WEISS (U.S. Patent No. 4,998,279).

VII. ARGUMENTS

A. The rejection under 35 U.S.C. § 103(a) based on BUFFAM (U.S. Patent No. 6,185,316) in view of KANEVSKY et al. (U.S. Patent No. 5,897,616) should be reversed.

A proper rejection under 35 U.S.C. § 103 requires that three basic criteria be met. First, there must be some suggestion or motivation, either in the references themselves, or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest *each and every claim feature*. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not the applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Appellant respectfully submits that the cited combination of BUFFAM and KANEVSKY et al. do not to disclose or reasonably suggest the combination of features recited in claim 1.

1. Claims 1-3 and 5.

Independent claim 1 recites a method of validating a user for a transaction to be effectuated by using a transaction card. The method includes configuring a biometric profile for said user, the biometric profile including a plurality of biometric samples received from the user, where the plurality of biometric samples correspond to a plurality of questions. The biometric profile is associated with an indicium assigned to said transaction card. The user is biometrically interrogated when the transaction is attempted by the user, where the biometrical interrogation includes querying the user for a biometric response associated with a randomly selected one of the plurality of questions. The biometric response generated with respect to said user in response to the biometrical interrogation is monitored and it is determined if the biometric response matches a biometric sample in the biometric profile corresponding to the randomly selected one of said plurality of questions. If so, the user is approved for the transaction. The combination of BUFFAM and KANEVSKY et al. does not disclose or reasonably suggest the combination of features recited in claim 1.

For example, BUFFAM and KANEVSKY et al. do not disclose or suggest the feature of querying the user for a biometric response associated with a randomly selected one of the plurality of questions, as recited in claim 1. The Examiner admits that BUFFAM does not disclose or suggest querying the user for a response associated with a randomly selected one of the plurality of biometric samples (Office Action – pg. 3). The Examiner cites KANEVSKY et al. to remedy this deficiency. Appellant respectfully submits that KANEVSKY et al. likewise does not disclose or reasonably suggest the recited feature.

In making the rejection, the Examiner relied on col. 3, lines 28-32 and 39-44 of KANEVSKY et al. for allegedly disclosing matching voice samples taken from answers to random questions (Office Action – pg. 3). Moreover, in addressing Appellant's prior remarks, the Examiner indicated that KANEVSKY et al. teaches determining if a biometric sample corresponds to the randomly selected question (final Office Action, dated February 21, 2006 – pg. 2). Appellant respectfully submits that this section of KANEVSKY et al. does not disclose or suggest querying the user for a response associated with a randomly selected one of the plurality of questions, where the questions correspond to a plurality of biometric samples stored in the user's profile, as required by claim 1.

At col. 3, lines 28-44, KANEVSKY et al. discloses:

> …(d) querying the speaker with at least one random (but questions could be non-random) question (but preferably more than one random question) based on the information contained in the accessed database; (e) receiving second spoken word utterances of the speaker, the second spoken utterances being representative of at least one answer to the at least one random question; (f) decoding the second spoken utterance; (g) verifying the accuracy of the decoded answer against the information contained in the accessed database serving as the basis for the question; (h) taking a voice sample from the utterances of the speaker and processing the voice sample against an acoustic model attributable to the speaker candidate; (i) generating a score corresponding to the accuracy of the decoded answer and the closeness of the match between the voice sample and the model…

This section of KANEVSKY et al. discloses using random questions to elicit a user voice response that is then analyzed for accuracy and compared to an acoustic model attributable to the user. In analyzing the voice response for accuracy, the voice response is decoded and the decoded answer is compared to non-biometric or non-acoustic information stored in a database (see, e.g., col. 10, lines 18-52 and element 18 in Fig. 1). In comparing the voice response to an acoustic model, the voice response is processed

against a predefined model that is *entirely unrelated to the random questions asked of the user*. In neither instance is a biometric response of a user compared to a biometric sample corresponding to a question randomly asked of the user. Consequently, KANEVSKY et al. teaches directly away from the invention as recited in independent claim 1. KANEVSKY et al. clearly discloses that speaker recognition and authentication processes are performed independently, so as to allegedly increase the security of the disclosed system. Clearly, KANEVSKY et al. does not disclose eliciting a response associated with a randomly selected one of a plurality of questions *corresponding to a plurality of biometric samples received from the user during configuration*.

It should be noted that KANEVSKY et al. is silent with respect to the specific manner in which the acoustic model is generated. However, the generated model is clearly not the source for the randomly selected questions, since this is retrieved from an accessed database and is referenced as a non-acoustic database. Moreover, this section of KANEVSKY et al. clearly indicates that a single acoustic model is compared against the received sample and that the acoustic comparison is conducted separately from the accuracy portion of the analysis. Furthermore, KANEVSKY et al. discloses that conventional voice recognition (not voice authentication) is initially performed to determine question accuracy (see, e.g., col. 6, lines 34-65). Following an accuracy determination, the received sample is compared against a previously built user model (see, e.g., col. 6, line 66 – col. 7, line 14). Clearly, KANEVSKY et al. does not disclose eliciting a response associated with a randomly selected one of a plurality of questions, where the questions correspond to a plurality of biometric samples received from the user

during configuration. For at least the foregoing reasons claim 1 is patentable over the cited combination of BUFFAM and KANEVSKY et al.

Claims 2, 3, and 5 depend from claim 1 and are therefore patentable over BUFFAM and KANEVSKY et al. for at least the reasons set forth above with respect to claim 1. Reconsideration and withdrawal of the pending rejections are respectfully requested.

B. The rejection under 35 U.S.C. § 103(a) based on BUFFAM (U.S. Patent No. 6,185,316) in view of KANEVSKY et al. (U.S. Patent No. 5,897,616), and further in view of FUJIMOTO et al. (U.S. Patent No. 5,893,057) should be reversed.

1. Claim 4.

Claim 4 depends from claim 1. Appellant respectfully submits that the disclosure of FUJIMOTO et al. does not remedy the deficiencies of BUFFAM and KANEVSKY et al. as set forth above with respect to claim 1. Therefore, claim 4 is patentable over the cited combination of BUFFAM, KANEVSKY et al., and FUJIMOTO et al. for at least reasons similar to those given above with respect to claim 1.

C. The rejection under 35 U.S.C. § 103(a) based on BUFFAM (U.S. Patent No. 6,185,316) in view of KANEVSKY et al. (U.S. Patent No. 5,897,616), and further in view of GLAZE et al. (U.S. Patent No. 6,320,974) should be reversed.

1. Claims 6 and 7.

Claims 6 and 7 depend from claim 1. Appellant respectfully submits that the disclosure of GLAZE et al. does not remedy the deficiencies of BUFFAM and KANEVSKY et al. as set forth above with respect to claim 1. Therefore, claims 6 and 7

are patentable over the cited combination of BUFFAM, KANEVSKY et al., and GLAZE et al. for at least reasons similar to those given above with respect to claim 1.

D. The rejection under 35 U.S.C. § 103(a) based on BUFFAM (U.S. Patent No. 6,185,316) in view of KANEVSKY et al. (U.S. Patent No. 5,897,616), and further in view of SAWYER et al. (U.S. Patent No. 6,324,271) should be reversed.

1. Claims 8 and 10.

Independent claim 8 recites a method of validating a user for a call to be effectuated over a Public Switched Telephone Network (PSTN) using a calling card. The method includes configuring a personalized profile for said user, said personalized profile including a plurality of voice samples elicited from said user in response to a plurality of personalized questions directed to said user; associating said personalized profile with an indicium assigned to said calling card; determining if a voice verification is needed with respect to said user when said call is attempted by said user; if so, querying said user for a voice response to a question that is randomly selected from said plurality of personalized questions; verifying if said voice response matches a corresponding voice sample in said voice profile; and if so, approving said user for said call involving said calling card. The cited combination of BUFFAM, KANEVSKY et al., and SAWYER et al. do not disclose or suggest the combination of features recited in claim 8.

For example, BUFFAM, KANEVSKY et al., and SAWYER et al. do not disclose or suggest querying said user for a voice response to a question that is randomly selected from said plurality of personalized questions, as recited in claim 8. In particular, the Examiner admits that BUFFAM does not disclose or suggest querying said user for a voice response to a question that is randomly selected from said plurality of personalized

questions (Office Action – pg. 5). The Examiner cites KANEVSKY et al. to remedy this deficiency. Appellant respectfully submits that KANEVSKY et al. likewise does not disclose or reasonably suggest the recited feature.

In making the rejection, the Examiner relied on col. 3, lines 28-32, and 39-44 of KANEVSKY et al. for allegedly disclosing matching voice samples taken from answers to random questions (Office Action – pg. 5). Appellant respectfully submits that this section of KANEVSKY et al. does not disclose or suggest querying said user for a voice response to a question that is randomly selected from said plurality of personalized questions, where the questions correspond to a plurality of voice samples stored in the user's personalized profile, as required by claim 8.

At col. 3, lines 28-44, KANEVSKY et al. discloses:

> …(d) querying the speaker with at least one random (but questions could be non-random) question (but preferably more than one random question) based on the information contained in the accessed database; (e) receiving second spoken word utterances of the speaker, the second spoken utterances being representative of at least one answer to the at least one random question; (f) decoding the second spoken utterance; (g) verifying the accuracy of the decoded answer against the information contained in the accessed database serving as the basis for the question; (h) taking a voice sample from the utterances of the speaker and processing the voice sample against an acoustic model attributable to the speaker candidate; (i) generating a score corresponding to the accuracy of the decoded answer and the closeness of the match between the voice sample and the model…

This section of KANEVSKY et al. discloses using random questions to elicit a voice response from a user. The received voice response may then be separately analyzed for 1.) accuracy and 2.) its closeness to an acoustic model attributable to the user. As further evidenced at col. 10, lines 18-52, it would appear that the system of KANEVSKY et al. queries the user for information included within a database associated with the user. This database is constructed of non-acoustic information (see, e.g., element 18 in Fig. 1). An

acoustic response to a presented question is compared against a separately generated acoustic model. The acoustic model does not correspond *in any way* with the question posed to the user for authentication. Rather, KANEVSKY et al. clearly discloses that speaker recognition and authentication processes are performed independently, so as to allegedly increase the security of the disclosed system. Clearly, KANEVSKY et al. does not disclose eliciting a response associated with a from said plurality of personalized questions, where the questions correspond to a plurality of voice samples stored in the user's personalized profile.

It should be noted that KANEVSKY et al. is silent with respect to the specific manner in which the acoustic model is generated. However, the generated model is clearly not the source for the randomly selected questions, since this is retrieved from an accessed database and is referenced as a non-acoustic database. Moreover, this section of KANEVSKY et al. clearly indicates that a single acoustic model is compared against the received sample and that the acoustic comparison is conducted separately from the accuracy portion of the analysis. Furthermore, KANEVSKY et al. discloses that conventional voice recognition (not voice authentication) is initially performed to determine question accuracy (see, e.g., col. 6, lines 34-65). Following an accuracy determination, the received sample is compared against a previously built user model (see, e.g., col. 6, line 66 – col. 7, line 14). Clearly, KANEVSKY et al. does not disclose from said plurality of personalized questions, where the questions correspond to a plurality of voice samples stored in the user's personalized profile during configuration. For at least the foregoing reasons claim 8 is patentable over the cited combination of BUFFAM and KANEVSKY et al.

The disclosure of SAWYER et al. does not remedy the deficiencies of BUFFAM and KANEVSKY et al. For at least these reasons, claim 8 is patentable over the cited combination of BUFFAM, KANEVSKY et al., and SAWYER et al.

Claim 10 depends from claim 8 and is therefore patentable over BUFFAM, KANEVSKY et al., and SAWYER et al. for at least the reasons set forth above with respect to claim 8.

2. Claim 9.

Claim 9 depends from claim 8. Accordingly, claim 9 is therefore patentable over BUFFAM, KANEVSKY et al., and SAWYER et al. for at least the reasons set forth above with respect to claim 8. Moreover, claim 9 includes additional features neither disclosed nor suggested by the cited combination.

For example, claim 9 recites populating at least a portion of the personalized profile with a plurality of DTMF samples responses elicited from the user in the configuration step, and prompting the user to input a DTMF response in response to the question that is randomly selected from the plurality of personalized questions. None of the cited references disclose or reasonably suggest this combination of features.

In making the rejection the Examiner indicates that the combination of BUFFAM and KANEVSKY et al. do not disclose using DTMF responses to answer random questions (Office Action – pg. 5). To remedy this deficiency, the Examiner cited col. 7, lines 53-60 of SAWYER et al. as allegedly disclosing using DTMF to answer random questions (Office Action – pg. 6). Appellant respectfully disagrees.

Col. 7, lines 53-60 of SAWYER et al. discloses:

> To accommodate existing DTMF telephones, an alternative embodiment of CCID is described in which the dialling of a conventional telephone calling card number and PIN, or the dialling of a calling card number followed by the dialling of a time varying PIN displayed on a suitable cryptographic token, would result in a CCID call. The certification method used for the call would be communicated to the terminating end as a certification level number following the reserved CCID indicator that precedes the caller's name in a CCID call.

This section of SAWYER et al. discloses using DTMF to facilitate reception of a calling card number and PIN to authenticate a caller. This section of SAWYER et al. does not disclose or even remotely suggest populating at least a portion of the personalized profile with a plurality of DTMF samples responses elicited from the user in the configuration step, and prompting the user to input a DTMF response in response to the question that is randomly selected from the plurality of personalized questions. Additionally, the Examiner has provided no motivational basis for the allegedly proper combination of SAWYER et al. with the previous combination of BUFFAM and KANEVSKY et al. For at least these reasons, Appellant submits that the rejection of claim 9 under 35 U.S.C. §103(b) is improper. Reconsideration and allowance of claim 9 are respectfully requested.

E. The rejection under 35 U.S.C. § 103(a) based on BUFFAM (U.S. Patent No. 6,185,316) in view of KANEVSKY et al. (U.S. Patent No. 5,897,616), further in view of SAWYER et al. (U.S. Patent No. 6,324,271), and still further in view of FUJIMOTO et al. (U.S. Patent No. 5,893,057) should be reversed.

1. Claim 11.

Claim 11 depends from claim 8. Appellant respectfully submits that the disclosure FUJIMOTO et al. do not remedy the deficiencies of BUFFAM, KANEVSKY et al., and SAWYER et al. as set forth above with respect to claim 8. Therefore, claim 11

is patentable over the cited combination of BUFFAM, KANEVSKY et al., SAWYER et al., and FUJIMOTO et al. for at least reasons similar to those given above with respect to claim 8.

F. The rejection under 35 U.S.C. § 103(a) based on BUFFAM (U.S. Patent No. 6,185,316) in view of SAWYER et al. (U.S. Patent No. 6,324,271), further in view of CHMAYTELLI et al. (U.S. Patent No. 6,542,729), and further in view of WEISS (U.S. Patent No. 4,998,279) should be withdrawn.

1. Claims 12-15.

Appellant proposed the cancellation of claims 12-15 in the After-Final Amendment filed April 20, 2006. Although this Amendment was not entered, Appellant does not wish to present arguments regarding the patentability of these claims at this time. Accordingly, cancellation of claims 12-15 without prejudice or disclaimer and withdrawal of the pending rejection thereto, are respectfully requested.

G. The rejection under 35 U.S.C. § 103(a) based on BUFFAM (U.S. Patent No. 6,185,316) in view of KANEVSKY et al. (U.S. Patent No. 5,897,616), further in view of SAWYER (U.S. Patent No. 6,324,271), and further in view of WEISS (U.S. Patent No. 4,998,279) should be reversed.

1. Claims 16-22.

Independent claim 16 recites an access control system for use with a transaction-card-based scheme. The access control system includes a network operable with a terminal, where the terminal interacts with a user in association with a transaction card. A controller is disposed in the network to query the user when the user attempts a

transaction using the transaction card. A server is disposed in the network to respond to messages from the controller with respect to querying the user. A profile database is coupled to the server, the profile database having a plurality of biometric samples inherently coupled to the user, where the plurality of biometric samples relate to a plurality of questions, and where the biometric samples are associated with an indicium assigned to the transaction card such that when the user attempts the transaction, the controller queries the user for a response relating to a randomly selected one of the biometric samples and if the response does not match a corresponding entry in the profile database, access is denied to the user for the transaction. The cited combination of BUFFAM, KANEVSKY et al., SAWYER et al., and WEISS does not disclose or reasonably suggest each and every feature of claim 16.

In rejecting claim 16, the Examiner fails to address the specific features recited in the claim. Accordingly, a *prima facie* case of obviousness has not been established with respect to claim 16. More specifically, in rejecting claim 16, the Examiner indicated that the combination of BUFFAM, KANEVSKY et al., SAWYER et al., and WEISS allegedly disclose "a method of validating a user for a transaction by using a transaction card" (Office Action – pg. 8). Claim 16 is not directed to a method of validating a user for a transaction by using a transaction card, but rather to an access control system for use with a transaction-card-based scheme. Moreover, the substance of the Examiner's entire rejection fails to address the specific features recited in claim 16.

For example, the rejection of claim 16 alleges that BUFFAM discloses configuring a biometric profile for a user including a plurality of biometric samples at col. 18, lines 18-35 and 57-63 (Office Action – pg. 8). Claim 16 does not recite

configuring a biometric profile for a user including a plurality of biometric samples. Instead, claim 16 recites a profile database coupled to said server, said profile database having a plurality of biometric samples inherently coupled to said user, wherein said plurality of biometric samples relate to a plurality of questions.

Similarly, the rejection of claim 16 alleges that BUFFAM discloses biometrically interrogating said user when said transaction is attempted at col. 18, line 65 to col. 19, line 2 (Office Action – pg. 8). Claim 16 does not recite biometrically interrogating said user when said transaction is attempted. Instead, claim 16 recites a network operable with a terminal, said terminal for interacting with a user in association with a transaction card; and a controller disposed in the network to query said user when said user attempts a transaction using said transaction card.

The rejection of claim 16 further alleges that KANEVSKY discloses receiving spoken answers in response to submitted questions, and verifying the user and the answers via a database at col. 3, lines 26-44 (Office Action – pg. 8). Claim 16 does not recite receiving spoken answers in response to submitted questions, and verifying the user and the answers via a database. Instead, claim 16 recites that the controller queries the user for a response relating to a randomly selected one of the biometric samples and if the response does not match a corresponding entry in the profile database, access is denied to the user for the transaction.

For at least this reason, Appellant submits that the Examiner has failed to establish a *prima facie* case of obviousness with respect to claim 16. Even assuming, *arguendo*, that BUFFAM, KANEVSKY et al., SAWYER et al., and WEISS have been properly applied in the rejection of claim 16, (a point that Appellant does not concede),

Appellant respectfully submits that the cited combination does not disclose or suggest a controller that queries the user for a response relating to a randomly selected one of the plurality of biometric samples, wherein the plurality of biometric samples relate to a plurality of questions, as required by claim 16.

The Examiner alleged that SAWYER et al. discloses a network operable with a terminal in association with a transaction card (Office Action – pg. 8), but acknowledged that BUFFAM and SAWYER et al. do not disclose or suggest this feature and relied on col. 3, lines 26-44 of KANEVSKY et al. for allegedly disclosing receiving spoken answers in response to submitted questions, and verifying the user and the answers via a biometric database (Office Action – pg. 8). Appellant respectfully submits that this section of KANEVSKY et al. does not disclose or suggest a controller that queries the user for a response relating to a randomly selected one of the plurality of biometric samples, wherein the plurality of biometric samples relate to a plurality of questions, as recited by claim 16.

As recited above, col. 3, lines 26-44 of KANEVSKY et al. discloses using random questions to elicit a voice response from a user. The received voice response may then be separately and independently analyzed for 1.) accuracy and 2.) its closeness to an acoustic model attributable to the user. As evidenced at col. 10, lines 18-52, KANEVSKY et al. discloses that its system queries a user for information included within a non-acoustic database associated with the user. An acoustic response to a presented question is then compared against a single separately generated acoustic model. The acoustic model does not correspond *in any way* to the question posed to the user for authentication. Rather, KANEVSKY et al. clearly discloses that speaker recognition and

authentication processes are performed independently, so as to allegedly increase the security of the disclosed system. This section of KANEVSKY et al. does not disclose or suggest a controller that queries the user for a response relating to a randomly selected one of the plurality of biometric samples, wherein the plurality of biometric samples relate to a plurality of questions, as required by claim 16.

In fact, as noted above, KANEVSKY et al. is silent with respect to the specific manner in which the acoustic model is generated. However, the generated model is clearly not the source for the randomly selected questions, since this is retrieved from an non-acoustic user database. Moreover, this section of KANEVSKY et al. clearly indicates that a single acoustic model is compared against the received sample and that the acoustic comparison is conducted separately from the accuracy portion of the analysis. Furthermore, KANEVSKY et al. discloses that conventional voice recognition (not voice authentication) is initially performed to determine question accuracy (see, e.g., col. 6, lines 34-65). Following an accuracy determination, the received sample is compared against a previously built user model (see, e.g., col. 6, line 66 – col. 7, line 14). KANEVSKY et al. does not disclose a controller that queries the user for a response relating to a randomly selected one of the plurality of biometric samples, wherein the plurality of biometric samples relate to a plurality of questions. The cited WEISS reference does not remedy the noted deficiencies with respect to the BUFFAM, SAWYER et al., and KANEVSKY et al. references, as noted above.

For at least the foregoing reasons, Appellant submits that the rejection of claim 16 under 35 U.S.C. § 103(a) based on BUFFAM, KANEVSKY et al., SAWYER et al., and WEISS is improper. Accordingly, Appellant requests that the rejection be reversed.

Claims 17-22 depend from claim 16. Therefore, Appellant submits that claims 17-22 are patentable over BUFFAM, KANEVSKY et al., SAWYER et al., and WEISS for at least the reasons given above with respect to claim 16.

VIII. CONCLUSION

In view of the foregoing arguments, Appellants respectfully solicit the Honorable Board to reverse the Examiner's rejections of claims 1-11 and 16-22 under 35 U.S.C. § 103.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY SNYDER, L.L.P.

By: /Robin C. Clark/
Robin C. Clark
Registration No. 40,956

Date: March 28, 2007

11350 Random Hills Road
Suite 600
Fairfax, Virginia 22030
(571) 432-0800

Customer No. 25537

IX. CLAIM APPENDIX

1. A method of validating a user for a transaction to be effectuated by using a transaction card, comprising:

configuring a biometric profile for said user, said biometric profile including a plurality of biometric samples received from the user, the plurality of biometric samples corresponding to a plurality of questions;

associating said biometric profile with an indicium assigned to said transaction card;

biometrically interrogating said user when said transaction is attempted by said user, wherein said biometrical interrogation includes querying said user for a biometric response associated with a randomly selected one of said plurality of questions;

monitoring said biometric response generated with respect to said user in response to the biometrical interrogation;

determining if said biometric response matches a biometric sample in said biometric profile corresponding to the randomly selected one of said plurality of questions; and

if so, approving said user for said transaction.

2. The method of validating a user for a transaction as set forth in claim 1, wherein at least a portion of said plurality of biometric samples comprises voice samples generated by said user responsive to a plurality of questions directed to said user in said

configuring step, and further wherein said biometrical interrogation involves querying said user for a voice response to a randomly selected question of said plurality of questions.

3. The method of validating a user for a transaction as set forth in claim 1, further comprising:

prompting said user to input said indicium assigned to said transaction card after determining that said biometric response matches a biometric sample of said biometric profile;

determining if said indicium is a valid personal identification number operating as a password associated with said transaction card; and

denying access to said user for said transaction if said indicium is not a valid personal identification number associated with said transaction card.

4. The method of validating a user for a transaction as set forth in claim 1, further comprising:

prompting said user to input said indicium assigned to said transaction card if said biometric response does not match a biometric sample of said biometric profile;

confirming that said indicium is a valid personal identification number associated with said transaction card; and

approving said user for said transaction upon said confirmation.

5. The method of validating a user for a transaction as set forth in claim 1, wherein

configuring a biometric profile for said user is effectuated manually.

6. The method of validating a user for a transaction as set forth in claim 1, wherein configuring a biometric profile for said user is effectuated automatically.

7. The method of validating a user for a transaction as set forth in claim 1, further comprising updating said biometric profile for said user.

8. A method of validating a user for a call to be effectuated over a Public Switched Telephone Network (PSTN) using a calling card, comprising:

configuring a personalized profile for said user, said personalized profile including a plurality of voice samples elicited from said user in response to a plurality of personalized questions directed to said user;

associating said personalized profile with an indicium assigned to said calling card;

determining if a voice verification is needed with respect to said user when said call is attempted by said user;

if so, querying said user for a voice response to a question that is randomly selected from said plurality of personalized questions;

verifying if said voice response matches a corresponding voice sample in said voice profile; and

if so, approving said user for said call involving said calling card.

9. The method of validating a user for a call as set forth in claim 8, further comprising:

populating at least a portion of said personalized profile with a plurality of Dual Tone Multi Frequency (DTMF) sample responses elicited from said user in said configuration step;

prompting said user to input a DTMF response in response to said question that is randomly selected from said plurality of personalized questions;

verifying if said DTMF response matches a corresponding sample response in said personalized profile; and

denying access to said user for said call if said DTMF response does not match said corresponding sample response in said personalized profile.

10. The method of validating a user for a call as set forth in claim 8, further comprising:

prompting said user to input said indicium assigned to said calling card after verifying that said voice response matches a corresponding voice sample in said voice profile;

determining if said indicium is a valid personal identification number associated with said calling card; and

denying access to said user for said call if said indicium is not a valid personal identification number associated with said calling card.

11. The method of validating a user for a call as set forth in claim 8, further

comprising:

prompting said user to input said indicium assigned to said calling card after verifying that said voice response does not match a corresponding voice sample in said voice profile;

confirming that said indicium is a valid personal identification number associated with said calling card; and

approving said user for said call upon said confirmation.

12. A fraud prevention method for use in a transaction-card-based system having a conventional authentication process, comprising:

determining, by utilizing said conventional authentication process, if a fraudulent transaction is being attempted in said transaction-card-based system by a user using a transaction card;

if so, biometrically interrogating said user to obtain a biometric sample from said user; and

upon obtaining said biometric sample, denying access to said user for said transaction in said transaction-card-based system if said biometric sample does not match an entry stored in a biometric profile database inherently associated with said transaction card's owner, wherein the biometric profile database includes a plurality of biometric samples previously received from the user.

13. The fraud prevention method for use in a transaction-card-based system as set forth in claim 12, wherein said fraudulent transaction is selected from the group

comprising: placing a calling card call, accessing personal information data, accessing a bank account, accessing an Internet account, accessing a credit report, accessing employment records, and accessing medical records.

14. The fraud prevention method for use in a transaction-card- based system as set forth in claim 12, wherein said entry inherently associated with said transaction card's owner comprises a voiceprint associated with said owner.

15. The fraud prevention method for use in a transaction-card-based system as set forth in claim 12, wherein said entry inherently associated with said transaction card's owner comprises at least one of a fingerprint, retinal scan, palm print, and implanted ID chip associated with said owner.

16. An access control system for use with a transaction-card- based scheme, said system comprising:

a network operable with a terminal, said terminal for interacting with a user in association with a transaction card;

a controller disposed in the network to query said user when said user attempts a transaction using said transaction card;

a server disposed in the network, said server responding to messages from said controller with respect to querying said user; and

a profile database coupled to said server, said profile database having a plurality of biometric samples inherently coupled to said user, wherein said plurality of biometric

samples relate to a plurality of questions, and wherein said biometric samples are associated with an indicium assigned to said transaction card such that when said user attempts said transaction, said controller queries said user for a response relating to a randomly selected one of the biometric samples and if said response does not match a corresponding entry in said profile database, access is denied to said user for said transaction.

17. The access control system for use with a transaction-card-based scheme as set forth in claim 16, wherein said entry inherently coupled to said user comprises at least one of a fingerprint, retinal scan, palm print, and implanted ID chip associated with said user.

18. The access control system for use with a transaction-card-based scheme as set forth in claim 16, wherein said entry inherently coupled to said user comprises a voiceprint associated with said user.

19. The access control system for use with a transaction-card-based scheme as set forth in claim 16, wherein said controller comprises an Automated Response Unit associated with a Public Switched Telephone Network.

20. The access control system for use with a transaction-card-based scheme as set forth in claim 16, wherein said terminal comprises a wireline phone.

21. The access control system for use with a transaction-card based scheme as set forth in claim 16, wherein said terminal comprises an Internet phone.

22. The access control system for use with a transaction-card-based scheme as set forth in claim 16, wherein said terminal comprises a wireless medium device.

X. EVIDENCE APPENDIX

None.

XI. RELATED PROCEEDINGS APPENDIX

None.